Yale Law School
Yale Law School Legal Scholarship Repository

Lecturer and Other Affiliate Scholarship Series | Yale Law School Other Scholarship

2-6-2011

When Machines Are Watching: How Warrantless Use of GPS Surveillance Technology Terminates The Fourth Amendment Right Against Unreasonable Search

Priscilla Smith
Yale Law School, priscilla.smith@yale.edu

Nabiha Syed

Albert Wong

David Thaw

Follow this and additional works at: http://digitalcommons.law.yale.edu/ylas

Part of the Civil Rights and Discrimination Commons, Constitutional Law Commons, Criminal Law Commons, and the Science and Technology Commons

Recommended Citation
Smith, Priscilla; Syed, Nabiha; Wong, Albert; and Thaw, David, "When Machines Are Watching: How Warrantless Use of GPS Surveillance Technology Terminates The Fourth Amendment Right Against Unreasonable Search" (2011). *Lecturer and Other Affiliate Scholarship Series.* Paper 2.
http://digitalcommons.law.yale.edu/ylas/2

This Article is brought to you for free and open access by the Yale Law School Other Scholarship at Yale Law School Legal Scholarship Repository. It has been accepted for inclusion in Lecturer and Other Affiliate Scholarship Series by an authorized administrator of Yale Law School Legal Scholarship Repository. For more information, please contact julian.aiken@yale.edu.

When Machines Are Watching: How Warrantless Use of GPS Surveillance Technology Terminates The Fourth Amendment Right Against Unreasonable Search

©*Priscilla J. Smith, Nabiha Syed, David Thaw, Albert Wong*[1]

Abstract: The use of GPS surveillance technology for prolonged automated surveillance of American citizens is proliferating, and a direct split between the Ninth and D.C. Circuits on whether warrants are required under the Fourth Amendment for such use of GPS technology is bringing the issue to a head in the Supreme Court. A Petition for Certiorari is pending in the Ninth Circuit case which held that warrants are not required, and a second Petition is likely from the Government in the D.C. Circuit case holding that warrants are required. In this paper, we argue first, that where a technology enables invasion of interests at the heart of the Fourth Amendment's concern -- protection of citizens from arbitrary government intrusions into their private lives -- the Court's precedents require warrants to prevent abuse, and second, that the type and scope of information collected by prolonged automated GPS surveillance enables governments to monitor a person's political associations, their medical conditions and their amorous interests, in a way that invades their privacy and chills expression of other fundamental rights.

Our argument differs significantly from previous scholarship by tracing a continuous emphasis in Fourth Amendment jurisprudence on review of the potential for abuse of surveillance methods. Moreover, we are the first to argue that in protecting against abuse the Court has drawn a firm line between technology

---

[1] The authors are Fellows of the Information Society Project at Yale Law School (ISP), an intellectual center addressing the implications of new information technologies for law and society. Priscilla Smith is a Senior Fellow of the ISP, with a focus on reproductive rights, privacy law, information policy and new technologies. Smith litigated cases concerning constitutional rights to liberty, privacy and freedom of speech for 13 years at the Center for Reproductive Rights. She holds a J.D. from Yale Law School and a B.A. from Yale College. Nabiha Syed is a Marshall Scholar at Oxford University researching comparative freedom of information laws. Syed holds a J.D. from Yale Law School, a B.A. from Johns Hopkins, and is the author of "Replicating Dreams" (Oxford University Press, 2008). Albert Wong is a Ph.D. student in Cell Biology at Yale University, holds a S.M. in Health Sciences and Technology from MIT, and an Honors B.S. from the University of Texas at Arlington. Wong has published multiple peer-reviewed articles in engineering and biology, and is supported by an NIH National Research Service Award. David Thaw is a Ph.D. candidate in Information Management and Systems at Berkeley, holds a J.D. from Berkeley Law, an M.A. in Political Science from Berkeley, and a B.S. (Computer Science) and B.A. (Government) from the University of Maryland. Thaw practiced information privacy law in Washington, D.C., and has published articles and book chapters based on his research in information security and spyware. He will join the University of Maryland Computer Science faculty in spring 2011.

that simply *enhances* the *natural* senses of law enforcement officials, and technology that *creates* novel, *non-biological* "senses."

In Part I of this paper, we trace the origins of the Fourth Amendment's protections against law enforcement abuse, present evidence that GPS surveillance technology is in fact being abused, and discuss the impact unfettered abuse of the technology will have on the individual rights of citizens. In Part II, we explain the Court's historic approach to new surveillance technologies, noting that the Court has carefully examined new technologies to prevent any end-runs around legal doctrine from eroding personal privacy, and showing that the Court has always required warrants where technology goes beyond enhancement of senses to the creation of new non-biological "senses." In Part III, we explain why the Supreme Court's ruling on the use of beeper technology *to enhance* visual surveillance in *United States v. Knotts*, 460 U.S. 276 (1983), does not apply to the use of GPS technology as a *replacement for* visual surveillance. Finally, in Part IV, we explain how prolonged automated GPS surveillance invades a reasonable expectation of privacy and chills the exercise of core constitutional rights.

Table of Contents

Introduction 3

I. Fundamental Principles of The Fourth Amendment Require Application of the Warrant Requirement to Prevent Abuse of GPS Surveillance Technology. 7

II. Historically, The Court Has Prevented New Surveillance Technologies From Encroaching Fundamental Constitutional Values 13

III. The Court's Ruling in *Knotts* Does Not Apply to the Use of GPS Surveillance Technology for Prolonged, Automated Surveillance 19

IV. Warrantless Prolonged GPS Surveillance Invades a Reasonable Expectation of Privacy and Will Chill the Exercise of Core Constitutional Rights.....21

a. GPS surveillance technology is more intrusive than primitive beeper technology in constitutionally significant ways 22

b. GPS surveillance technology is not in general public use. 24

CONCLUSION.....26

INTRODUCTION

When used properly, advanced surveillance technologies significantly enhance the ability of law enforcement to maintain order and public safety. However, in an era of rapidly advancing technologies, from thermal imagers to minuscule automated tracking devices, it is critical to ensure that these technologies, especially given their advanced capabilities, are only used "in a manner which will conserve … the interests and rights of individual citizens," *Kyllo v. United States,* 533 U.S. 27, 40 (2001) (internal citation omitted), and preserve core Fourth Amendment values. Although the United States Supreme Court has held that in most cases, "requiring a warrant will have the salutary effect of ensuring that use of [new technology] is not abused," *see United States v. Karo*, 468 U.S. 705, 717 (1984), federal and many State law enforcement officials throughout the nation are currently using Global Positioning System ("GPS") surveillance technology for prolonged, automated, remote surveillance without obtaining warrants.

As a result, cases are proliferating in which law enforcement's warrantless uses of GPS surveillance technology are being challenged by defendants, and courts are looking for direction from the Supreme Court. Most recently, a split has emerged between the Ninth and D.C. Circuits on the issue. In *United States v. Pineda-Moreno*,[2] the Ninth Circuit relied on *United States v. Knotts*, 460 U.S. 276, 283-94 (1983) -- which approved limited use of relatively primitive beeper technology -- to

[2] 591 F.3d 1212 (9th Cir. 2010), *reh'g en banc denied*, 617 F.3d 1120 (9th Cir. 2010), Petition for Certiorari, No. 10-1715, (filed Nov. 10, 2010).

uphold warrantless use of the vastly more complex GPS surveillance technology.[3] On the other hand, in *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), *reh'g en banc denied*, 625 F.3d 766 (D.C. Cir. 2010), the D.C. Circuit pointed to the vast differences between the limited use of beepers to enhance visual surveillance almost thirty years ago in *Knotts* and the unprecedented power of GPS surveillance technology used today and held that warrants are required.[4]

State courts are similarly divided. On the one hand, high courts in three states -- Washington, New York, and Massachusetts -- held that warrants are required for use of GPS under the state's constitution, and the Supreme Court of Oregon held that warrants are even required for the use of beepers, a far less powerful electronic monitoring device.[5] On the other hand, three state intermediate appellate courts -- in Virginia, Wisconsin and Maryland – have held that a warrant is not required for

---

[3] The Seventh Circuit has suggested in dicta that a warrant may not be required for the use of GPS. *See United States v. Garcia,* 474 F.3d 994, 998 (7th Cir. 2007). However, the appellant in that case had not challenged the use of GPS to track his car on public streets, but only the installation of the GPS device itself, and even the dicta is based on the court's belief that GPS was not being used in "routine criminal enforcement," but only when the police "have a suspect in their sights," and an appropriate level of suspicion. *Id.*; *see also Maynard,*615 F.3d at 557 (discussing *Garcia* and citing Br. of Appellant at 22 (No. 06-2741)). Moreover, in *Garcia* Judge Posner warned "Technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive," and expressed with relief that "Whether and what kind of restrictions should, in the name of the Constitution, be placed on such surveillance when used in routine criminal enforcement are momentous issues that fortunately we need not try to resolve in this case."

[4] *See also* Chief Judge Kozinski's powerful dissent from denial of rehearing en banc in *Pineda-Moreno*, 617 F.3d 1120, 1126 (Kozinski, C.J., dissenting).

[5] *See People* v. *Weaver*, 909 N.E.2d 1195, 1201-03 (N.Y. 2009) (holding that state constitution requires a warrant for the use of GPS for prolonged law enforcement surveillance, and that issue was unresolved under Fourth Amendment to the U.S. Constitution); *Commonwealth* v. *Connolly*, 913 N.E.2d 356, 366 (Mass. 2009) (same); *State* v. *Jackson*, 76 P.3d 217, 264 (Wash. 2003) (en banc) (citizens of this State have a right [under the Washington State Constitution] to be free from the type of governmental intrusion that occurs when a GPS device is attached to a citizen's vehicle); *see also State* v. *Campbell*, 759 P.2d 1040 (Or. 1988) (use of radio transmitter was search requiring warrant under state constitution).

use of GPS.[6] The Supreme Court of Nevada has held that a warrant is not required for the use of the less-intrusive beeper technology when used as an aid to visual surveillance, but has not yet addressed the use of GPS for prolonged automated surveillance.[7]

In this paper, we argue that prolonged surveillance using GPS technology should be subject to the warrant requirement *under current Supreme Court precedent* for two reasons.[8] First, because surveillance with GPS is conducted *not by people* but by minuscule, advanced tracking devices communicating with satellites in orbit, the potential for law enforcement abuse of GPS technology to conduct automated and prolonged surveillance both against individuals as well as groups of individuals is unprecedented. Evidence exists that such abuse is occurring. Where a technology enables invasion of interests at the heart of the Fourth Amendment's concern -- protection of citizens from arbitrary government intrusions into their private lives -- the Court's precedents require warrants to prevent abuse.

---

[6] *See Foltz* v. *Commonwealth*, 698 S.E.2d 281, 290 (Va. Ct. App. 2010) (holding no warrant required for use of GPS "for at most six days"); *State* v. *Sveum*, 769 N.W.2d 53, 60 (Wis. Ct. App. 2009) (no warrant required for use of GPS for law enforcement surveillance under U.S. Constitution); *Stone* v. *State*, 941 A.2d 1238, 1250-51 (Md. Ct. Spec. App. 2008) (holding that "appellant did not have a reasonable expectation of privacy in his location . . . in a vehicle riding on public roads, and therefore evidence about the use of the GPS device . . . was not relevant to the appellant's Fourth Amendment-based suppression motion.").

[7] *Osburn* v. *State*, 44 P.3d 523, 525-26 (Nev. 2002) (en banc) (holding only that no warrant was required for use of a *beeper* as an aid to visual surveillance under Nevada Constitution)

[8] Another commentator has argued that current Fourth Amendment jurisprudence would need to be modified to take the potential for abuse of surveillance techniques into account. *See* Brian J. Serr, Great Expectations of Privacy: A New Model for Fourth Amendment Protection, 73 MINN. L. REV. 583, 623 (1989) (the proper inquiry *should be* whether abuse of method would reduce privacy).

Second, we argue that prolonged surveillance using GPS technology provides the government with detailed information about an individual's movements and gathering places and allows the storage, analysis, and comparison of that data with data gathered from others, all with minimal involvement of law enforcement officers. The type and scope of information collected by GPS surveillance enables governments to monitor a person's political associations, their medical conditions, and their amorous interests, in a way that invades their privacy and chills expression of other fundamental rights. *See NAACP v. Alabama,* 357 U.S. 449 (1958) (forced disclosure of names of members of NAACP violated right to freedom of association protected by federal Constitution). It allows surveillance of citizens on a scale that this country has never seen. *United States v. Pineda-Moreno*, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing *en banc*) (making comparison to surveillance under a totalitarian regime).

In Part I of this paper, we trace the origins of the Fourth Amendment's protections against law enforcement abuse, present evidence that GPS surveillance technology is in fact being abused, and discuss the impact unfettered abuse of the technology will have on the individual rights of citizens. In Part II, we explain the Court's historic approach to new surveillance technologies, noting that the Court has carefully examined new technologies to prevent any end-runs around legal doctrine from eroding personal privacy. Furthermore, the Court has drawn a firm line between technology that simply *enhances* the *natural* senses of law enforcement

officials, and technology that *creates* novel, *non-biological* "senses," requiring warrants for the latter. In Part III, we explain why the Supreme Court's ruling on the use of beeper technology *to enhance* visual surveillance in *Knotts* does not apply to the use of GPS technology as a *replacement for* visual surveillance. Finally, in Part IV, we explain how prolonged automated GPS surveillance invades a reasonable expectation of privacy and will chill the exercise of core constitutional rights. We conclude by arguing that the Supreme Court should clarify that while law enforcement may employ advanced GPS tracking devices in their efforts to enhance public safety, use of this technology for prolonged, automated, remote surveillance is subject to the Fourth Amendment's protections of a warrant issued by a neutral arbiter on probable cause.

I. Fundamental Principles of The Fourth Amendment Require Application of the Warrant Requirement to Prevent Abuse of GPS Surveillance Technology.

The Fourth Amendment provides our primary protection against "a too permeating police surveillance" and abuse of police authority, *United States v. Di Re*, 332 U.S. 581, 595 (1948), and "gives concrete expression to a right of the people which 'is basic to a free society.'" *Camara v. Mun. Ct. of City & Cty. of San Francisco*, 387 U.S. 523, 528 (1967). *See also Byars v. United States*, 273 U.S. 28, 33-34 (1927). In response to "indiscriminate searches and seizures conducted under the authority of 'general warrants,'" *Payton v. New York*, 445 U.S. 573, 583 & n. 21 (1980), the Founders designed the Fourth Amendment to protect "the privacy and

security of individuals" against such "arbitrary invasions." *Camara*, 387 U.S. at 528 (1967) (citations omitted).

By placing a check on abuses of power, the Fourth Amendment also reflects a "deeply felt belief that the criminal law cannot be used as an instrument of unfairness, and that the possibility of unfair and even brutal police tactics poses a real and serious threat to civilized notions of justice." *Schneckloth v. Bustamonte*, 412 U.S. 218, 225 (1973). The Founders recognized that certain individuals are more at risk than others when they gather to discuss politics or transact business. To limit "discretion" and protect against police abuse, the Fourth Amendment requires that "the usual inferences which reasonable men draw from evidence" be drawn "by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime." *Payton*, 445 U.S. at 621 n.24. Without a warrant requirement, GPS technology increases exponentially the potential for surveillance abuse.[9]

There is a vast technical valley between the primitive beeper technology that the Court considered almost thirty years ago, and the advanced, automated GPS surveillance technology in use today. The beeper devices were simple tools that were approved for use without a warrant only when they provided modest sense-enhancement to real-time visual surveillance conducted by law enforcement officers. As described in *Knotts*, 460 U.S. at 277, "[a] beeper is a radio transmitter, usually

[9] *See Whalen v. Roe*, 429 U.S. 589, 606-07 (1977) (Brennan, J., concurring) (warning that "accessibility of computerized data vastly increase[s] the potential for abuse").

battery operated, which emits periodic signals that can be picked up by a radio receiver." After receiving the signal, whose strength indicates whether the object to which the beeper is attached is approaching or moving away, police officers *in the vicinity* could use this information to respond accordingly. *Id.* Beepers could neither determine location themselves nor store that data. *Pineda-Moreno*, 617 F.3d at 1124 (Kozinski, C.J., dissenting) ("If no one was close enough to pick up the signal, [the data] was lost forever.").

In contrast, modern GPS surveillance technology is a satellite-based service generally consisting of: 1) a GPS receiver (the "tracking device"), generally minuscule and inexpensive, that autonomously calculates latitude, longitude, altitude, direction and speed by receiving and processing location information from the transmissions of at least four GPS satellites in nearby orbit; 2) a wireless transmitter attached to the receiver which sends the calculated location information to a specified remote destination; and 3) a law enforcement computer that records the transmitted tracking data, stores it for an unlimited amount of time, and can analyze and compare it with data collected from other targets.[10,11] The first item comprises the "core" location-determining technology used in GPS surveillance; the second and third items are technologies to collect and process that location information for law enforcement use. Alternate methods of retrieving this

---

[10] *See Tied Up*, 55 UCLA L. Rev. at 415.

[11] *See U.S. Department of Defense, Global Positioning System Standard Positioning Service Performance Standard* 4th ed. at v (Sept. 2008), *available at* http://www.pnt.gov/public/docs/2008/spsps2008.pdf (last visited Feb. 3, 2011); *see also* GPS.gov *Frequently Asked Questions*, http://www.gps.gov/support/faq/ (last visited Feb. 3, 2011).

information exist, such as the use of digital storage onboard the GPS device to store the information and the subsequent retrieval of that information by manually accessing the device or via short-duration or "burst" wireless transmissions which can be triggered on-demand when an officer is within range to receive them. Thus, the requirement that law enforcement officers actively maintain proximity to the surveillance device – a notable limitation of "beeper" and other similar transponder-based location systems – is not present when using GPS surveillance.

GPS, unlike the beepers of yore, does not enhance human senses; it *replaces* them with something different in kind and capacity, allowing remote, automated collection of data about a target's location, movements, speed of movement, and even altitude. With GPS, time can be figured to within a millionth of a second, velocity within a fraction of a mile per hour, and location to within 1-2 meters of horizontal accuracy and 5 meters of vertical accuracy.[12] Efforts are underway to further improve accuracy to within 10-15 *centimeters.*[13]

Evidence is growing that the increasing availability of GPS surveillance

---

[12] *See Report to Congress: Recapitalization Plan for the NDGPS, U.S* DEPARTMENT OF TRANSPORTATION *(June 2010), available at ; U.S. Air Force, Global Positioning System, available at (describing system available in 92% of the contiguous U.S.);* Jim Arnold, High Accuracy Nationwide Differential Global Positioning System (HA-NDGPS) Update (Sept. 2009), *available at* http://www.navcen.uscg.gov/pdf/cgsicmeetings/49/Reports/%5B38%5DHA_NDGPS.pdf (last visited Feb. 4, 2011); Gary Pruitt, ARINC Incorporated, NDGPS Assessment: Final Report (March 2008), *available at* http://www.navcen.uscg.gov/pdf/ndgps/ndgps%20assessment%20report_final.pdf (last visited Feb. 4, 2011); *U.S. Department of Defense, Global Positioning System Standard Positioning Service Performance Standard* 4th ed. (Sept. 2008), *available at* http://www.pnt.gov/public/docs/2008/spsps2008.pdf (last visited Feb. 3, 2011) at v; *see also* test data available from the U.S. Dep't of Transportation's Wide Area Augmentation System, http://www.nstb.tc.faa.gov/.

[13] *See* GPS.gov *Augmentation Systems,* available at http://www.gps.gov/systems/ augmentations/ (last visited Feb. 3, 2011).

technology has led to abuse of law enforcement's power to monitor Americans to prevent and investigate criminal activity. The precise scope of GPS surveillance is unknown; there are no nationwide statistics available on the frequency of GPS surveillance and most police departments resist disclosing how often they use it. However, the FBI provides special training to its officers in the use of GPS[14] and some local jurisdictions have willingly reported the scope of their use.[15] For example, one police department, in Fairfax, Virginia, reports using GPS surveillance 61 times in 2005 alone.[16] A spokesperson for the National Association of Criminal Defense Lawyers reports that GPS surveillance has been used "in cases from New York City to small towns – whoever can afford to get the equipment and plant it on a car."[17]

In one recent incident, a twenty-year-old college student from Santa Clara, California, Yasir Afifi, discovered a GPS surveillance device affixed to his car. Afifi is an American citizen whose father, also an American citizen, was a former president of a Muslim Community Association in San Francisco before he moved to Egypt in 2003. Forty-eight hours after Afifi removed the device and asked for help online to identify it, he received a visit from several FBI agents who demanded the

---

[14] Keith Hodges, *Tracking Bad Guys: Legal Considerations in Using GPS*, Federal Bureau of Investigation Law Enforcement Bulletin (July 2007), *available at* http://www.fletc.gov/training/programs/legal-division/downloads-articles-and-faqs/articles/FBI-LE-Bulletin-GPS-Tracking-Jul2007.pdf/view?searchterm=GPS (last visited Feb. 3, 2011).
[15] Ben Hubbard, *Police Turn to Secret Weapon: GPS Device*, Washington Post (Aug.13, 2008), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/08/12/AR2008081203275.html (last visited Feb. 3, 2011).
[16] *Id.;* see also *Foltz* v. *Commonwealth*, 698 S.E.2d 281, 284 n.3 (Va. Ct. App. 2010).
[17] *Id.*.

return of the device. Afifi was then questioned about an online blog maintained by his close friend. To date, he has not been charged with a crime. The FBI, after reclaiming the tracking device, has provided no further details.[18]

Our freedom has depended in part on the government's inability to continually follow all, or even large groups, of us at any time for any reason. Because resources are limited, we know that the police cannot assign an officer to track each of us around the clock. Now, though, because the GPS satellite system can support an effectively unlimited number of tracking devices, and because GPS surveillance technology is inexpensive and allows automated tracking, neither cost nor limitations on human resources imposes an impediment to pervasive surveillance of the populace.[19]

As the Court has recognized, the only other effective limitation on abuse of surveillance tactics is the warrant requirement.[20] Without warrants, the police could track each and every one of us, or perhaps some large group of us, all Republicans, all Democrats, all Tea Party members, all those with Muslim surnames, for an unlimited amount of time, discovering our political beliefs, our medical maladies, and any other affairs we wished to keep to ourselves. This "too

---

[18] Kim Zetter, *Caught Spying on Student, FBI Demands GPS Tracker Back*, WIRED (Oct. 7, 2010), http://www.wired.com/threatlevel/2010/10/fbi-tracking-device/all/1 last visited Feb. 3, 2011).

[19] GPS surveillance technology "can provide law enforcement with a swift, efficient, silent, invisible and *cheap* way of tracking the movements of virtually anyone and everyone they choose." *Pineda-Moreno*, 617 F.3d at 1126 (Kozinski, C.J., dissenting).

[20] Enforcement depends upon the exclusionary rule as "neither administrative, criminal nor civil remedies are effective in suppressing lawless searches and seizures." *Elkins v. United States*, 364 U.S. 206, 217, 218, 220 (1960).

permeating police surveillance," *see Di Re*, 332 U.S. at 595, would serve as a crime deterrent; but it would also have a devastating effect, chilling free speech and association[21] and the expression of other desires essential to dignity and the pursuit of happiness.[22]

Used without a warrant requirement, GPS, like wiretaps, thermal imaging, and beepers used for more than sense-enhancement, "shrink[s] the realm of personal privacy," *Kyllo,* 533 U.S. at 34, beyond the dreams or nightmares of the Founders. Warrants would ensure that this powerful technology is not abused. *See Karo*, 468 U.S. at 717 (warrants prevent abuse of technology).

II. Historically, The Court Has Prevented New Surveillance Technologies From Encroaching Fundamental Constitutional Values.

Because new technologies can create powers of surveillance that were not anticipated when old legal standards were developed, the Court evaluates them to "assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo*, 533 U.S. at 34.[23] The Court rejects "mechanical" application of standards that allow end-runs around Fourth Amendment protections, leaving us "at the mercy of advancing technology." *See id.*

---

[21] *See NAACP*, 357 U.S. at 462.

[22] *See Lawrence v. Texas,* 539 U.S. 558, 574 (2003) ("'intimate and personal choices . . . [are] central to personal dignity") (quoting *Planned Parenthood v. Casey*, 505 U.S. 833, 851 (1992)).

[23] Means of surveillance, not only results, determine whether a form of investigation or inquiry is acceptable. *Kyllo*, 533 U.S. 37-39; *Whalen*, 429 U.S. at 606-07 (Brennan, J., concurring) (Fourth Amendment limits not only "the type of information the State may gather," but also "the means it may use to gather it."); *Schmerber v. California*, 384 U.S. 757, 767 (1966) ("overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the state.").

at 36. Instead, the Court encourages adoption of rules that "take account of more sophisticated systems that are already in use or in development." *Id.* at 37. As the Court cautioned more than eighty years ago:

> the assurance against any revival of [police abuse], so carefully embodied in the fundamental [Fourth Amendment] law, is not to be impaired by judicial sanction of equivocal methods, which, regarded superficially, may seem to escape the challenge of illegality but which, in reality, strike at the substance of the constitutional right.

Byars, 273 U.S. at 33-34.

Accordingly, the Court's decisions examine whether allowing a new surveillance method to be used unfettered by the modest limitations of the warrant requirement, and therefore subject to officer "discretion" and abuse, will diminish privacy in ways antithetical to the aims of a free society. *Kyllo,* 533 U.S. at 34-36. *See also NAACP*, 357 U.S. at 462 (recognizing vital connection between constitutional rights to privacy and freedom of association). The Court has not hesitated to modify its Fourth Amendment inquiry as necessary to ensure the original meaning of the Amendment is carried forward.

For example, in *Katz v. United States*, 389 U.S. 347 (1967), the Court evaluated law enforcement's use of listening devices allowing them to eavesdrop on a target's phone conversations even when attached to the *outside* of phone booths. The officers could listen to the conversation as if the device was inside the room, all while meeting the technical requirements of Fourth Amendment doctrine that at the time prohibited only *physical* intrusion into the private sphere. *See Olmstead v.*

United States, 277 U.S. 438 (1928). The Court modified the doctrine to fit new realities, recognizing that the difference between physical and electronic intrusion had "no constitutional significance." *Katz*, 389 U.S. at 353. The Court held that the Fourth Amendment protects "people, not places," *id.* at 361, and emphasized that notions of privacy and improper intrusion protected by the Fourth Amendment cannot be defeated by technological developments allowing end runs around previous doctrine. *Id.* at 362.[24]

In a similar vein, in *Schmerber v. California*, where the Court faced "intrusions into the human body rather than . . . state interferences with property relationships or private papers-'houses, papers, and effects'," it "wr[o]te on a clean slate." 384 U.S. at 767-68. Though the Court ultimately approved the search in *Schmerber* under the exigent circumstances exception, this new more intrusive method of search garnered additional scrutiny from the Court.

In addition, while the Court has approved of some primitive "sense-enhancing" technologies to aid officers conducting visual surveillance, the Court has placed limits on their use. The Court has *never* allowed unwarranted use of "sense-creating" technologies – those that do not enhance human senses but operate independently of humans. Indeed, the *Knotts* holding is part of a tradition of

[24] The protections of the Fourth Amendment go beyond the walls of each man's "castle." *See, e.g.,* Osmond K. Fraenkel, *Concerning Searches and Seizures*, 34 HARV. L. REV. 361, 365 (1921); *Stanley v. Georgia,* 394 U.S. 557, 564 (1969) (Founders also "protect[ed] Americans in their beliefs, their thoughts, their emotions and their sensations.") (quoting *Olmstead v. United States*, 277 U.S. 438, 478 (Brandies, J., dissenting)).

allowing the limited use of primitive technologies as sense-enhancements of, *not as replacements for*, visual surveillance; the Court has always required warrants for the use of technologies that replace human senses with technological ones. *See Kyllo,* 533 U.S. at 40 (thermal imaging); *Karo*, 468 U.S. at 717 (beepers when used as alternative to visual surveillance); *Katz v. United States*, 389 U.S. 347 (1967) (wiretapping); *Walter v. United States*, 447 U.S. 649 (1980) (movie projector).

For example, in *United States v. Lee*, 274 U.S. 559, 563 (1927), the Court confirmed that no search took place where officers used "searchlights" or "marine glass or field glass" to help them see on the deck of a ship. *See also Dow Chemical Co.*, 476 U.S. at 237-38 (warrantless use of airplane-mounted camera authorized because "mere fact that human vision is enhanced somewhat, at least to the degree here, does not give rise to constitutional problems"). In contrast, in *Walter v. United States*, 447 U.S. 649 (1980), the Court held that using a movie projector, fairly basic technology even at the time, to view films without a warrant was an unreasonable search under the Fourth Amendment. The projector didn't just "enhance" sight, it created a new capacity. The police would have been unable to discern the content of a film strip, *id.* at 652 n.2, even with a bright light or a magnifying glass. The use of a technology that gave them the new ability to inspect the strip's contents required warrant authorization. *Id.* at 654. *See also Katz*, 389 U.S. at 353.[25]

[25] It is doubtful that a warrant would have been required in *Katz* if the police had merely listened to the conversation through the wall of the phone booth using a glass placed backwards to enhance the noise.

Knotts, like *Lee*, is a simple application of the "sense-enhancement" rule. The Court upheld the use of beepers without a warrant where they were being used as "sense-augmenting" technology that merely enhanced visual surveillance.[26] As the Court wrote in referencing the searchlights and marine and field glass at issue in *Lee*, "[n]othing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case." *Knotts*, 460 U.S. at 282-83 (quoting *United States v. Lee,* 274 U.S. 559, 563 (1927)).

United States v. Karo, decided one year later, makes clear the limitations of the *Knotts* decision. The Court held that a warrant *was* required for monitoring and downloading beeper data when the beeper was in "a location not open to visual surveillance," and "reveal[ed] a critical fact about the interior of the premises that Government . . . could not have otherwise obtained without a warrant." 468 U.S. at 714-15. Thus, as with the movie projector in *Walter*, when the beeper does not enhance human senses but creates a new sense, a warrant is required.

In *Kyllo*, the Court again demonstrated the limitations of the "sense-enhancement" exception. The Court recognized that it had "previously reserved judgment as to how much technological enhancement of ordinary perception . . . if any, is too much." 533 U.S. at 33. The Court held that use of thermal-imaging

[26] In *Knotts*, after obtaining consent, officers placed a beeper within a container to be purchased by the suspect. *Knotts*, 460 U.S at 278. They did so only after visual surveillance indicated suspicion. Moreover, officers only used the beeper to maintain contact with the container of chloroform in the vehicle itself. *Knotts*, 460 U.S. at 282.

technology to obtain "any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion" constituted a search "at least where (as here) the technology in question is not in general public use." *Id.* at 34. While finding the thermal-imaging technology at issue there "relatively crude," the Court in *Kyllo* advocated adopting a rule that could "take account of more sophisticated systems that are already in use or in development." *Id.* at 36. At some point, the Court warned, technology might not just enhance human senses by allowing us to see and hear from farther distances or in the dark, but could actually create new superhero-like powers, like X-ray vision, *see id.* at 36 n.3, or perhaps the ability to watch thousands of people using satellites. If law enforcement had at its disposal the ability to use these non-human powers of surveillance without any warrant limitation, law enforcement technology would "shrink the guaranteed realm of privacy." *See Kyllo*, 533 U.S. at 34.

The Ninth Circuit erred in viewing the key distinction between *Kyllo* (warrant required) and *Knotts* (warrant not required) as the fact that the thermal imaging technology in *Kyllo* gathered information that would otherwise have been obtained only by "a search unequivocally within the meaning of the Fourth Amendment," *Pineda-Moreno*, 591 F.3d at 1216, in other words a search of the home. But if the officers had merely discovered evidence by looking into the home from outside the house with their bare eyes, or even with eyesight enhanced by binoculars, they would also have been gathering information that could otherwise only be obtained

by a search of the home subject to the warrant requirement, yet *that* surveillance would have been allowable without a warrant, because the technology (binoculars) would have been allowable "sense-enhancing" technology.[27]

In *Kyllo*, the Court's discomfort was with the use of a technology that actually went beyond "enhancement" of senses. The use of a technology capable of obtaining images of heat by itself created a new sense, *substituting for* human senses. *Id.* at 36 n.3. This is the fundamental distinction between *Knotts* on the one hand (warrant not required) and *Kyllo*, *Katz*, *Walter,* and GPS surveillance technology on the other (warrant required).

III. The Court's Ruling in *Knotts* Does Not Apply to the Use of GPS Surveillance Technology for Prolonged, Automated Surveillance.

The Ninth Circuit was wrong to rely on *Knotts* to support its ruling for three reasons. First, as discussed above, the decision in *Knotts* was limited to situations where beepers were used as a "sense-enhancement" technology. *Knotts*, 460 U.S. at 282; *id.* at 283 (noting "limited use" which government made of signals from beeper); *id.* at 284-85 (beeper signal not received or relied on after it indicated that container ended journey). GPS surveillance technology does not involve "sense-enhancement," but rather substitution for human senses and therefore should be governed by *Katz, Kyllo* and *Walter,* not *Knotts*.

[27] The Court rejected as "quite irrelevant" the dissent's objection that heat emanating from the home can sometimes be perceived by observers without the use of technology. *Id.* at 35, n. 2 ("The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment.").

Second, in *Knotts* the Court reserved the question presented by GPS surveillance technology. *Id.* at 283-84; *see also United States v. Maynard*, 615 F.3d 544, 556 (D.C. Cir. 2010) ("the [*Knotts*] Court specifically reserved the question whether a warrant would be required in a case involving 'twenty-four hour surveillance.'").[28] As the D.C. Circuit noted:

> *Knotts* held only that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another," *id.* at 281, not that such a person has no reasonable expectation of privacy in his movements whatsoever, world without end, as the Government would have it.

Maynard, 615 F.3d at 557.[29] *See also Dow Chemical*, 476 U.S. at 238 ("[U]sing highly sophisticated surveillance equipment not generally available to the public, *such as satellite technology*, might be constitutionally proscribed absent a warrant.") (emphasis added).

Finally, the Ninth Circuit also erred in claiming that the Court's concern expressed in *Knotts* and *Kyllo* about technology allowing twenty-four hour surveillance was a concern limited to the potential for "mass" surveillance." While such a prospect is not to be taken lightly, in reserving the question the Court was referring to the defendant's concern that "twenty-four hour surveillance of *any citizen* of this country will be possible, without judicial knowledge or supervision."

---

[28] *See also Pineda-Moreno*, 617 F.3d at 1125-26 (Kozinski, C.J., dissenting).

[29] *See also People v. Weaver*, 12 N.Y.3d 433, 440-44 (2009) (*Knotts* involved a "single trip" and Court "reserved for another day the question of whether a Fourth Amendment issue would be posed if 'twenty-four hour surveillance of any citizen of this country [were] possible' "); *Tied Up,* 419 UCLA L. Rev. at 457.

Knotts, 460 U.S. at 283 (emphasis added); *see also Pineda-Moreno,* 617 F.3d at 1126 (Kozinski, C.J., dissenting); *Maynard*, 615 F.3d at 556-57.

On the other hand, there is nothing in the Ninth Circuit's decision that would prevent "mass" surveillance. Nor do we know whether the surveillance in that case was indeed part of a program of "mass" surveillance, not albeit of *everyone* in the United States but of some significant portion of the population.

IV. Warrantless Prolonged GPS Surveillance Invades a Reasonable Expectation of Privacy and Will Chill the Exercise of Core Constitutional Rights.

As the Court recognized in *Knotts*:

> this Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action. [Citations omitted].

Knotts, 460 U.S. at 280-81. In *Pineda-Moreno*, the Ninth Circuit relied on *Knotts* to hold that the government can use GPS surveillance technology without warrants because an individual has no reasonable expectation of privacy in his movements through public space. *Pineda-Moreno*, 591 F.3d at 1216-17. But not only is this a huge leap from the Court's more limited holding in *Knotts* that law enforcement may use primitive beeper technology as a sense-enhancement to aid in a search,[30] it also fails to recognize the intrusiveness of prolonged surveillance by invisible,

[30] *See also Pineda-Morena,* 617 F.3d at 1125-26 (Kozinski, C.J., dissenting).

automated devices that continuously gather and analyze detailed information about a person's movements for an unlimited period of time.[31]

a. GPS surveillance technology is more intrusive than primitive beeper technology in constitutionally significant ways.

Three aspects of GPS surveillance technology distinguish it from "sense-enhancing" beeper technology in constitutionally significant ways: its automated nature, the level of detail obtained, and its ability to store data for long periods and to analyze and compare it. First, once the GPS tracking device is installed, it can operate autonomously over a prolonged period, without human involvement, independently determining and remotely transmitting positional data. Unlike the beepers of yore, police officers need not trail the device or deploy a network of receivers in order to determine location information. As Chief Judge Kozinski puts it:

> Beepers could help police keep vehicles in view when following them, or find them when they lost sight of them, but they still required at least one officer--and usually many more--to follow the suspect. The modern devices used in Pineda-Moreno's case can record the car's movements without human intervention.

Pineda-Moreno, 617 F.3d at 1124 (Kozinski, C.J., dissenting). Since GPS tracking devices operate autonomously, no police officer experiences real-time "sense-enhancement" as is the case with a beeper, telescope or flashlight.

[31] *See Schmerber*, 384 U.S. at 767 (Fourth Amendment "protects personal privacy and dignity against unwarranted intrusion by the state.").

Second, GPS tracking devices "know" their own location and can be equipped to both store that information locally (on the device itself) and transmit that information (either in real-time or in bursts) to remote law enforcement computers. This flexibility represents a significant advance in location tracking, allowing collection of substantially more data and for prolonged periods. As the government recognizes elsewhere, GPS tracking devices are "more intrusive" than beeper-style transponders.[32] Thus, prolonged surveillance by GPS "reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble." *Maynard,* 615 F.3d at 562; *id.* at 560.[33]

Third, the electronic storage of gathered location data allows the data to be considered alongside data collected from other citizens to discover common patterns of behavior among different groups of people, a capability that beepers do not have. As Chief Judge Kozinski commented:

> By tracking and recording the movements of millions of individuals the government can use computers to detect patterns and develop suspicions. It can also learn a great deal about us because where we go says much about who we are. … Were Jones, Aaronson and Rutherford at that protest outside the White House?

Pineda-Moreno, 617 F.3d at 1125 (Kozinski, C.J., dissenting).

---

[32] *See Tracking Bad Guys* at 26.

[33] *In re Application of the United States for Historical Cell Site Data*, No. H-10-998M, 2010 WL 4286365 at *7-8 (S.D. Tex. Oct. 29, 2010) (historical cell phone records subject to Fourth Amendment under *Maynard* because records sought "are likely far more intrusive"; they reveal "a continuous reality TV show, exposing two months' worth of a person's movements, activities, and associations in relentless detail.").

b. GPS surveillance technology is not in general public use.

GPS surveillance technology is not in general public use, and as a result we *do* still have an expectation that we are not being followed perpetually by an invisible computerized eye in the sky. *See Kyllo*, 533 U.S. at 28. Many Americans are comfortable with use of a GPS service to determine their own personal location where that service operates subject to their consent and control.[34] GPS *surveillance* technology, however, is not accepted by the public. In fact, Americans become uncomfortable with GPS when there is even a slight loss of user-control.[35]

For example, despite a strong push by companies encouraging Americans to adopt "geosocial" software that would allow users to broadcast their locations to selected friends using GPS in their phones, only 4 percent of adult Americans use these services.[36] Americans are wary of anything that will take away our ability to preserve our anonymity in public. As Chief Judge Kozinski notes,

---

[34] Subscription services such as LoJack and OnStar can access an automobile's location and even transmit this location in case of emergency or theft, but only do so with the consent of the user. Contrary to Judge Posner's assertion in *Garcia*, Google Earth, the web service providing satellite images of the ground, cannot track people or vehicles in real time. *Compare United States v. Garcia,* 474 F.3d 994, 997 (7th Cir. 2007), with http://earth.google.com/support/bin/answer.py?hl=en&answer=176147 ("[t]he information in Google Earth is . . . not in 'real time'.").

[35] GPS technology is also used by some private and government employers to ensure job performance and service delivery, but this use is limited to the terms of the employment relationship and happens only while the employee is on the job using a vehicle owned by the employer. *See e.g.,* Judy Muller, *City Monitors Employees With GPS*, ABC News, Feb. 21 2004, *available at* http://abcnews.go.com/WNT/story?id=129219&page=1 (city governments use GPS tracking systems to ensure efficiency and monitor services such as street-sweeping and fixing potholes). *See* Nannette Green Kaminski and William Tran, The National Workrights Institute, *On Your Tracks: GPS Tracking in the Workplace* at 6, *available at* http://www.workrights.org/issue_electronic/NWI_GPS_Report.pdf.

[36] 4% OF ONLINE AMERICANS USE LOCATION-BASED SERVICES at 2 (PEW RESEARCH CENTER'S INTERNET AND AMERICAN LIFE PROJECT NOV. 4, 2010), *available at* http://pewinternet.org/Reports/2010/Location-based-services.aspx.

> You can preserve your anonymity from prying eyes, even in public, by traveling at night, through heavy traffic, in crowds, by using a circuitous route, disguising your appearance, passing in and out of buildings and being careful not to be followed.

617 F.3d at 1126 (Kozinski, C.J., dissenting).

In other contexts, the federal government recognizes that members of the American public maintain a reasonable expectation of privacy in data about their movements from place to place throughout the day. To recruit volunteers whose vehicles would be equipped with GPS devices for a federally-funded study to assess a new mileage-based tax, study organizers felt it necessary to assure volunteers that "[n]o detailed route information regarding your driving will be stored or collected," *Privacy of Information*, http://www.roaduserstudy.org/faq.aspx#privacy (last visited Dec. 5, 2010), and information about mileage would be maintained in "highly secure locations" in a separate database on a separate server from their personal information. *See id. & video available at* http://www.roaduserstudy.org/howitworks.aspx. (last visited Dec. 3, 2010).[37] If we did not have a reasonable expectation that such information would be private, organizers would not have felt the need to provide these assurances.

Indeed, any finding that individuals had come to expect that information about their every movement *is* being collected and stored for analysis would mean that a fundamental goal of the Founders had been abandoned. As the Court has

[37] *See National Evaluation of a Mileage-based Road User Charge*, UNIVERSITY OF IOWA PUBLIC POLICY CENTER, http://www.roaduserstudy.org/Default.aspx (last visited Dec. 5, 2010) (describing federal pilot program tracking vehicles with GPS).

recognized, there is a "vital relationship between freedom to associate and privacy in one's associations. . . . Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." *NAACP,* 357 U.S. at 462. "[W]rits of assistance and general warrants are but puny instruments of tyranny and oppression" when compared with the power of GPS surveillance technology. *See Olmstead*, 277 U.S. at 476 (Brandeis J., dissenting).

CONCLUSION

The Ninth Circuit's strained, "mechanical application" of *Knotts*, a case concerning sense-enhancing beeper technology, to the surveillance capabilities made possible by GPS surveillance technology leaves fundamental interests protected by the Fourth Amendment unguarded. Without a warrant requirement to guide its use, the potential for abuse of GPS surveillance technology is unprecedented and its use will significantly "shrink the realm of personal privacy." *See Kyllo,* 533 U.S. at 34. It is time for the United States Supreme Court to step in and clarify that as with other new technologies that allow machines to do the watching, GPS surveillance technology can only be used for prolonged automated surveillance on the authority of a warrant issued on probable cause.